We are hiring 3 Ph.D. students and 1 postdoc to work on cutting-edge research projects.

Topics

The open positions are on the following topics (detailed descriptions in the next pages):

1. Distributed Ledger Technologies for Internet Registries and Intrusion Detection Systems
2. Automation Protocols for Reputation-driven Industrial IoT Systems
3. Intent Based Networking: Cross-Layer Modeling and Signaling
4. Artificial Intelligence Algorithms and Protocols for Automating Connect-Compute Fabrics

Research environment

Research laboratory:
Computer Science and Communications department (CEDRIC; https://cedric.cnam.fr)

Research team:
Networks and IoT Systems (ROC – Réseaux et Objets Connectés; https://roc.cnam.fr)

Related collaborative projects:
H2020 AI@EDGE: European project on AI for beyond-5G networks, with 19 European partners.
ANR INTELLIGENTSIA: national project on network automation with Orange, Inria, Acklio, Aguila.

Location:
Paris, France - downtown district (le Marais), third arrondissement. 2 rue Conté, Paris, France.

Period

The contracts can start on January – April 2021. 36 months for Ph.D. students and 18 for postdoc.

Salary

PhD: appr. 24 000 € gross/year – 1 700 € net/month (before "prelevement à la source").
Postdoc: 32 000+ € gross/year – 2 200+ € net/month (before "prelevement à la source").

In addition, 50% of the public transportation subscription can be reimbursed.

Optional: teaching activities in French and/or English for up to 64 h/year, 2 650 €/year.

Requirements

Master/PhD degree in computer science, computer engineering, or telecommunications engineering.

Application

ASAP and no later than Nov. 22, 2020, send to perm-roc@cnam.fr your preferred subject(s) and:

- An up to date curriculum vitae on 2 or 3 pages, including names and contact information of 2 reference persons (professors or industrial tutors).
- University/engineering degree marks for the last 3 years.
- A 1-page motivation letter.
- Copy of the master thesis and/or internship report(s).

1 – PHD: Distributed Ledgers for Internet Registries and Intrusion Detection

Internet registries rely on data management systems that, while being geographically distributed, often maintain a level of centralization in the dissemination of registry information to final users. Many official and independent registries sustain the daily operations of the Internet, in terms of numbering and addressing, such as domain-name and routing locator resolutions, IP prefixes, Autonomous System numbers, sub-protocol types numbers, as well as registries that are managed independently from Internet organizations such as IP address blacklists. In this Ph.D. project, we will work on the precise challenge of securing the creation and usage of IP address blacklists for Intrusion Detection Systems (IDS), and its relationship with other Internet registries that may affect its operations.

The state of the art in IP blacklisting software is rich in independent initiatives. For instance, Fail2ban [1] is an IDS widly used on servers to prevent brute-force attacks: it monitors network traffic, usually by scanning log files of provided services and automatically ban any IP address showing inappropriate behavior (i.e. attempting to many login in a short time). Fail2ban is an efficient way to stop brute force attack but its main draw back is being only able to act after the attack has started (detection based approach); being able to share between different hosts the detected abusive IP address would allow others hosts to prevent the attacks even before they start. Projects like CrowdSec [2] or Turris Sentinel [3] address the sharing issue by providing a centralized server which gather information about abusive IP address and share it between participant hosts. Those approach act at the firewall level. Another approach [4] is to target the router level by providing BGP feed of abusive IP address still relying on a centralized server to gather information on abusive IP address.
[1-4] are example of operational systems relying on legacy database systems. Alternative proposals to use blockchain technology with IDS exist such as [5], which targets sharing of private data and alert information. In this Ph.D. project we will instead focus on banned address list approach and target their integration at any IP forwarding nodes, such as firewalls, BGP routers, and software switches.

We will study how to leverage on a Distributed Ledger Technology (DLT) for shared data storage to distribute lists of abusive IP addresses as soon as they are detected. DLTs such as blockchains provide a secure way to share information between a high number of independent nodes operating under different authorities, while ensuring high availability and immutability differently from centralized systems. The specificity of this data call for ad-hoc consensus protocols, to validate writing operations on the DLT and ensure different data consistency degrees. Indeed, while conventional public blockchain aim to be open, for IDS usages each actors might have different needs and policies requiring techniques like the Endorsement Policy feature [6]. Interconnection among DLTs managing different yet dependent registries, such as IP blacklists and routing locators, will be also investigated.

The objective is to design new DLT systems for sharing intrusion detection information taking into account the different needs of the actors while preventing malicious behaviors. The usage of different DLT data structures, namely blockchain and directed acyclic graph, will be evaluated in combination of different consensus polities to handle writing, consistency and writer classification aspects. The evaluation will be based on an experimental platform of IP forwarding nodes, in particularly using NetFPGA cards [7] to run a Smart-NIC implementing Firewall and BGP router network functions.

References

[1] Fail2Ban project: https://www.fail2ban.org
[2] Crowsec project: https://crowdsec.net
[3] Turris Sentinel project: https://view.sentinel.turris.cz
[4] Consolidated Blackhole BGP Communities (CBBC) tool: http://arneill-py.sacramento.ca.us/cbbc
[5] W. Meng et al., "When Intrusion Detection Meets Blockchain Technology: A Review," in IEEE Access, Vol. 6, pp. 10179-10188, 2018,
[6] M. Belotti et al., A Vademecum on Blockchain Technologies: When, Which and How. IEEE Communications Surveys and Tutorials, Vol. 21, No. 4, pp: 3796, 3838, 2019.
[7] M. Soelman et al., "Hyperledger Fabric: Evaluating Endorsement Policy Strategies in Supply Chains," IEEE Int. Conference on Decentralized Applications and Infrastructures (DAPPS), 2020.
[7] NetFPGA project : https://netfpga.org

2 - PHD: Automation Protocols for Reputation-driven Industrial IoT Systems

Novel Industry 4.0 environments adopt the digitalization and the interconnection of traditional industrial systems to increase resource efficiency, adaptability and reliability of production cyber-physical systems (CPSs). Industrial CPSs show multiple and evolving requirements coming from the industrial environment, the user or the system itself.

Notably, a key requirement is runtime computing system adaptability to align to environment states, monitored and learned through sensors data, and to take appropriate actions, through actuators. The CPS orchestration strategies include software components enabling to deploy in runtime to handle the data flow processing and forwarding, hence meeting the user/system requirements. Such dynamic management is critical and requires reconfiguration and self-organizing capabilities to ensure adaptability, flexibility and reliability while avoiding loss of critical industrial data. Moreover, the applications that need to be deployed for these novel CPSs may require to use a trusted environment depending on the sensitivity of the collected data. In CPS research, trust computing models measure trustworthiness between objects/devices; typically, multi-factor and multi-dimensional utility functions are used to express the security level offered by the CPS devices and their reputation.

While many existing works focus on the design of self-organizing industrial IoT networked systems by controlling the data processing and forwarding as [1, 2, 3], integrating hardware accelerators [4] or relying on Machine Learning (ML) techniques [5, 6], research works on trust management address either security or reputation of CPS without considering resilience and adaptive behavior, as in [7]. Thus, CPS security and reliability using ML, as well privacy are also studied in this area [8, 9]. On the other hand, other works [10, 11] studied the system's behavioral variations of a resource-constrained CPS to deploy self-adaptive software components to react to variable system states.

In this PhD project, we will work toward a self-adaptive software component systems approach that consider an assessed security level and the trust behavioral of the system, which is an aspect not yet clearly covered by the state of the art. In particular, we will work on how to evaluate the CPS trustworthiness based on a heterogeneous set of factors, including the environment learning logic needed for self-deployment of suitable software components. The research steps ahead are:

- Identify the features that characterize the CPS trustworthy and their dynamic variability
- Propose a multi-factor trust assessment algorithm for a dependable CPS.
- Propose novel protocols for autonomous reconfiguration and deployment of CPS components.

References

[1] X. Li et al., "A review of industrial wireless networks in the context of Industry 4.0", Wir. Netw. 23(1), 2017.
[2] C. Lucas-Estan, J. Gozalvez, "Load Balancing for Reliable Self-Organizing Industrial IoT Networks" IEEE Transactions on Industrial Informatics, Vol. 15, N°. 9, Sept. 2019.
[3] T. Rahman et al, "Efficient Edge Nodes Reconfiguration and Selection for the Internet of Things", IEEE Sensors Journal, Vol. 19, N°. 12, pp. 4672- 4679, June 15, 2019.
[4] T. Fanni et al., "Multi-Grain Reconfiguration for Advanced Adaptivity in Cyber-Physical Systems," 2018 Int. Conference on ReConFigurable Computing and FPGAs (ReConFig).
[5] HJ. Shin et al. "SVM-Based Dynamic Reconfiguration CPS for Manufacturing System in Industry 4.0", Wireless Communication Mobile Computing, Vol. 2018.
[6] K. Junejo et al., "Trustee: A Trust Management System for Fog-enabled Cyber Physical Systems" in IEEE Transactions on Emerging Topics in Computing, 2019, early access.
[7] H. Xia et al., "A Reputation-Based Model for Trust Evaluation in Social Cyber-Physical Systems," in IEEE Transactions on Network Science and Engineering, vol. 7, no. 2, 2020.
[8] F. Kriebel et al., "Robustness for Smart Cyber Physical Systems and Internet-of-Things: From Adaptive Robustness Methods to Reliability and Security for Machine Learning," ISVLSI 2018.
[9] G. Fink et al. *Security and privacy in cyber-physical systems: foundations, principles & applications*, Wiley.
[10] M. Afanasov, L. Mottola, C. Ghezzi, "Towards Context-Oriented Self-Adaptation in Resource-Constrained Cyberphysical Systems", in Computer Software and Applications Conference Workshops (COMPSACW), 2014.
[11] S. Zeadally et al., "Self-Adaptation Techniques in Cyber-Physical Systems (CPSs)" IEEE Access, vol. 7, pp. 171126-171139, 2019.

3 - PHD: Intent-Based Networking: Cross-Layer Modeling and Signaling

Intent-Based Networking (IBN) is a new paradigm arising in network management. It is driven by the possibility to leverage on network programming capabilities to implement service provisioning "intents". An IBN solution meets "What to achieve" requirements expressed by users through User-to-Network Interfaces (UNIs); it is meant to support business goals and translate them into policies.

The interaction of an IBN system with a programmable infrastructure happens using Northbound Interfaces (NBIs) at the resource level, but can be the result of a composite intent translation chain from the UNI to many NBIs. For instance, taking the rising software-defined Radio Access Network environment (using ORAN for radio resource scheduling and ONAP for the orchestration layer), IBN can appear with orchestration intents at the ONAP user interface, and at the ORAN resource scheduling level at the near-real time controller, by means of the ORAN NBIs named A1 in the specifications; and as many NBI as resources (link, computing) can be solicited by the orchestration layer, so intents at the orchestration layer have to be deployable at the resource layers with resource-level intents. The standpoint of this project is therefore that the IBN-driven service orchestration is implemented across multiple resource-level NBIs, similarly to information systems architectures.

Works at the state of the art declining the IBN framework to edge network infrastructure exist, such as [1] for vehicular applications; software-defined exchanges are defined therein as middleware for inter-layer IBN communications. A similar concept is used in [2,3] to consider the context for the IBN definition, touching several technical components. Techniques to identify and to process intents via context characteristics using artificial intelligence frameworks are studied in [1]. Nonetheless, a great confusion persists on the precise intent definition (different concepts are used to present intents: intentions, objectives, or else requirements) and its linkage with resource-level IBN configuration rules. For instance, major SDN controllers todays (e.g. ONOS, ODL) only very partially develop the IBN capabilities. Only in [2] context characteristics to define intents are clearly stated, such as traffic profile, required network function, device information. In this sense, AI and Machine Learning (ML) can help in defining methods to identify intentions and relevant context characteristics, to map them to an orchestration-level IBN process, then translated to resource-level IBN policies.

In this respect, the PhD project will address the following challenges:

- qualify the notion of intent in IBN, including its cross-layer implications in orchestration and resource-level systems, with a rigorous intent taxonomy that can be customized.
- define the context characteristics that should account by AI/ML processes or human-driven systems toward the definition of intents.
- design a cross-layer IBN framework with signaling requirements from UNI to NBI levels for expressing different network automation flavors (e.g., planning, real-time)
- experimentally show case the IBN signaling framework and its utility in network automation, using existing open networking software platforms.

References

[1] A. Singh et al., "Intent-Based Network for Data Dissemination in Software-Defined Vehicular Edge Computing". IEEE Transactions on Intelligent Transportation Systems, 1–9, 2020, early-access.
[2] D. Comer, A. Rastegatnia, "OSDF: An Intent-based Software Defined Network Programming Framework," 2018 IEEE 43rd Conference on Local Computer Networks (LCN).
[3] J. Pan, McElhannon, "Future Edge Cloud and Edge Computing for Internet of Things Applications". IEEE Internet of Things Journal 5 (1): 439–49, 2017.

4 - POSTDOC: Artificial Intelligence for Automating Connect-Compute Fabrics

This postdoc position is in the frame of the new H2020 ICT-52 5GPP AI@EDGE project starting on Jan. 1, 2020. The project involves 19 academic and industrial partners from 6 European countries.

The focus of the project is to work on the design of a connect-compute communication infrastructure fabric able to automate the reconfiguration and orchestration of a softwarized infrastructure making use of micro-services of edge network and service functions. The project will work toward the design and experimentation of a novel Connect-Compute Fabric for edge computing services leveraging on artificial intelligence. The solution will be adapted to four main use-cases:
– vehicle cooperative perception for safe driving and smart mobility;
– cybersecurity for large Industrial IoT environment;
– drone communications for AI-assisted infrastructures;
– in-flight data communications for entertainment services.

The candidate should:

- have proven expertise in at least one of the following areas:
    - application of machine learning to network and/or computing systems.
    - transport multipath forwarding protocols such as MP-TCP, MP-QUIC.
    - NetFPGA programming to execute network protocols and/or AI/ML algorithms.
    - Kubernetes, in-depth and hands-on experience of network and scaling primitives
- be fluent in both written and oral English.
- have proven high-quality publication record with at least 2 Q1 journal publications or very-high-impact contributions.
- show proven experience in collaborative multi-partner collaborative projects or larger internal projects.

The position is for a 18-month contract renewable once for additional 18 months.